	L #	Search Text	DBs	Time Stamp	Hits
1	L1	yamamoto.in. and hiroshi.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:03	14591
2	L2	ohdaira.in. and toshimitsu.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:03	15
3	L3	L1 and L2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:03	11

	L #	Search Text	DBs	Time Stamp	Hits
4	L4	sony.asn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:03	323695
5	L5	L3 and L4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:04	6
6	L6	713/167.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:04	416

	L #	Search Text	DBs	Time Stamp	Hits
7	L7	713/167.ccls. and "dummy code"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:04	0
8	L8	713/167.ccls. and "dummy data"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:04	1
9	L9	713/168.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:04	1910

	L #	Search Text	DBs	Time Stamp	Hits
10	L10	713/168.ccls. and (dummy (code or data))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:05	1879
11	L11	713/168.ccls. and (dummy code or data)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:05	1879
12	L12	380/201.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:05	1004

	L #	Search Text	DBs	Time Stamp	Hits
13	L13	380/201.ccls. and "dummy code"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:05	1
14	L14	380/201.ccls. and "dummy data"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:05	9
15	L15	380/44.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:06	907

	L #	Search Text	DBs	Time Stamp	Hits
16	L16	380/44.ccls. and "dummy code"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:06	2
17	L17	380/44.ccls. and "dummy data"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:06	2
18	L18	(encrypted) adj (protective object) near (protect code) near (executable module)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:07	0

	L #	Search Text	DBs	Time Stamp	Hits
19	L19	(encrypted) same(protective object) near (protect code) near (executable module)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:07	7
20	L20	(encrypted or enciphered or encoded) same (protective object) near (protect code) near (executable module)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:07	24
21	L21	(code) adj (writing) near (dummy data or dummy code) near (protect code)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:08	45

	L #	Search Text	DBs	Time Stamp	Hits
22	L22	L20 and L21	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:08	0
23	L23	(protect code) near (random number)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:08	51000
24	L24	L21 and L23	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:08	9

	L #	Search Text	DBs	Time Stamp	Hits
25	L25	L24 and L20	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/08/02 19:08	0

Interference Search

	L #	Search Text	DBs	Time Stamp	Hits
26	L26	encrypted AND protective AND object AND protect AND code.CLM.	US-PGPUB	2007/08/02 19:10	214
27	L27	encrypted AND protective AND object AND protect AND code AND storage AND encrypted.CLM.	US-PGPUB	2007/08/02 19:11	137
28	L28	encrypted AND protective AND object AND protect AND code AND storage AND encrypted AND invalidity.CLM.	US-PGPUB	2007/08/02 19:11	1
29	L29	encrypted AND protective AND object AND protect AND code AND storage AND encrypted AND decrypting.CLM.	US-PGPUB	2007/08/02 19:11	70
30	L30	encrypted AND protective AND object AND protect AND code AND storage AND encrypted AND decrypting AND code AND writing AND reading.CLM.	US-PGPUB	2007/08/02 19:11	42
31	L31	encrypted AND protective AND object AND protect AND code AND storage AND encrypted AND decrypting AND code AND writing AND reading AND executable AND module.CLM.	US-PGPUB	2007/08/02 19:11	11
32	L32	encrypted AND protective AND object AND protect AND code AND storage AND encrypted AND decrypting AND code AND writing AND reading AND executable AND module AND linking.CLM.	US-PGPUB	2007/08/02 19:12	2
33	L33	encrypted AND protective AND object AND protect AND code AND storage AND encrypted AND decrypting AND code AND writing AND reading AND executable AND module AND linking AND deleting.CLM.	US-PGPUB	2007/08/02 19:12	1

	Comments
26	
27	
28	
29	
30	
31	
32	
33	

	L #	Search Text	DBs	Time Stamp	Hits
34	L34	encrypted AND protective AND object AND protect AND code AND storage AND encrypted AND decrypting AND code AND writing AND reading AND executable AND module AND linking AND dummy AND data.CLM.	US-PGPUB	2007/08/02 19:12	4
35	L35	encrypted AND protective AND object AND protect AND code AND storage AND encrypted AND decrypting AND code AND writing AND reading AND executable AND module AND linking AND dummy AND data AND information AND processing.CLM.	US-PGPUB	2007/08/02 19:12	2

	Comments
34	
35	

Web Results **1 - 10** of about **60** for **dummy data, decrypt, protect code, encrypt, link "executable module"**. (

Did you mean: dummy data, decrypt, ***protected*** code, encrypt, link "executable module"

Information processing apparatus, **executable module** generating ...
The **executable module** is generated by generating, with **decryption** of an ..... 6, the **protect code** applying process unit may add a first **dummy data** area ...
www.freepatentsonline.com/20020032868.html - 78k - Cached - Similar pages

Communication system and security assurance device - Patent ...
United States Patent 20060048228 Kind **Code**: A1. **Link** to this page: ..... And the security assurance authority 2 appends the **encrypted data** which has been ...
www.freepatentsonline.com/20060048228.html - 170k - Cached - Similar pages

EP1182532 Sony european software patent - Information processing ...
6, the **protect code** applying process unit may add a first **dummy data** area 1 ..... the **encrypted protect code** contained in said **executable module** when said ...
gauss.ffii.org/PatentView/EP1182532 - 86k - Cached - Similar pages

Appendixes
DLL: Dynamic **Link** Library. An **executable module** containing functions that ..... A private key is also used to **decrypt** messages that were **encrypted** with the ...
publib.boulder.ibm.com/infocenter/txformp/v5r1/topic/com.ibm.txseries510.doc/aetga10072.htm - 172k - Cached - Similar pages

[PDF] OSF DCE Version 1.2.2 Release Notes
File Format: PDF/Adobe Acrobat - View as HTML
(with target build_all) to build the following **executable module**: ..... Add **Encryption/Decryption** Functions. Since the DFA source **code** shipped from OSF ...
support.entegrity.com/private/doclib/docs/osfdc122/dcern.pdf - Similar pages

[PDF] HP Open Source Security for OpenVMS Volume 1: Common **Data** Security ...
File Format: PDF/Adobe Acrobat
addition to the **encryption/decryption** CDSA calls. It **links** explicitly against ..... a dynamically loadable **executable module** (for example, DLL) to ...
h71000.www7.hp.com/doc/83final/BA554_90006/BA554_90006.pdf - Similar pages

[GZIP] PaCkAgE DaTaStReAm MAzip 1 496 # end of header ...
File Format: Gzip Archive - View as HTML
See the file 'WHERE' for access to the **encryption code**. **Decryption** can be made with unzip 5.0p1 or later, or with zipcloak. All bug reports or patches ...
ftp://ftp.sunfreeware.com/pub/freeware/intel/2.6/zip-2.2-sol26-intel-local.gz - Similar pages

Perl lietuviškai.
adaptive differential pulse **code** modulation - skirtuminis garso ..... **data** processing - duomenų apdorojimas **data protection** - duomenų apsauga ...
www.perl.lt/zodynas - 288k - Cached - Similar pages

[PDF] Temporary Binding for Dynamic Middleware Construction and Web ...

File Format: PDF/Adobe Acrobat
5.8 **Data Encryption/Decryption** using Public/Private Key . . . . . 87 ..... remote process

components are implemented as stand-alone **executable module ...**
www.hpi.uni-potsdam.de/fileadmin/hpi/Forschung/Publikationen/Dissertationen/Dissertation-Huang.pdf - Similar pages

O'Reilly Media -- Bookstore: C# Cookbook
There are many ways to write secure **code** and **protect data** using the . ... You have a string you want to be able to **encrypt** and **decrypt**—perhaps a password or ...
www.oreilly.com/catalog/csharpckbk/toc.html?CMP=ILL-4GV796923290 - Similar pages

Did you mean to search for: dummy data, decrypt, ***protected*** code, encrypt, link "executable module"

1 2 3 4 5 **Next**

Terms used:
executable module dummy data protect code decrypt encrypt

Found **24** of **207,474**

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 24 Result page: **1** 2 next

Relevance scale

1 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

2 Workshop papers: On instrumenting obfuscated java bytecode with aspects
Kung Chen, Ju-Bing Chen
May 2006 **Proceedings of the 2006 international workshop on Software engineering for secure systems SESS '06**
Publisher: ACM Press
Full text available: pdf(92.02 KB) Additional Information: full citation, abstract, references, citings, index terms

Code obfuscators are widely used tools for protecting commercial Java software. Advanced obfuscation techniques make de-compiled Java programs not re-compilable, thus greatly raising the barrier of instrumenting Java bytecode for malicious purpose. However, we have found that the aspect-oriented programming language AspectJ can be abused to overcome advanced code obfuscation and to modify obfuscated Java software effectively using its bytecode instrumentation mechanism. This paper describes such ...

Keywords: AspectJ, Java, aspect-oriented programming, code obfuscation, software protection

3 Software protection and simulation on oblivious RAMs

Oded Goldreich, Rafail Ostrovsky
May 1996 **Journal of the ACM (JACM)**, Volume 43 Issue 3
Publisher: ACM Press

Full text available: pdf(3.44 MB) Additional Information: full citation, abstract, references, citings, index terms

Software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper, we provide theoretical treatment of software protection. We reduce the problem of software protection to the problem of efficient simulation on oblivious RAM.A machine is oblivious if thhe sequence in wh ...

Keywords: pseudorandom functions, simulation of random access machines, software protection

4 Encryption-based protection for interactive user/computer communication

Stephen Thomas Kent
September 1977 **Proceedings of the fifth symposium on Data communications SIGCOMM '77**
Publisher: ACM Press

Full text available: pdf(846.33 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper develops a virtual connection model, complete with intruder, for interactive terminal-host communication and presents a set of protection goals that characterize the security that can be provided for a physically unsecured connection. Fundamental requirements for protocols that achieve these goals and the role of encryption in the design of such protocols are examined. Functional and security constraints on positioning of protection protocols in a communication system and the imp ...

5 (How) can mobile agents do secure electronic transactions on untrusted hosts? A survey of the security issues and the current solutions

Joris Claessens, Bart Preneel, Joos Vandewalle
February 2003 **ACM Transactions on Internet Technology (TOIT)**, Volume 3 Issue 1
Publisher: ACM Press

Full text available: pdf(197.96 KB) Additional Information: full citation, abstract, references, citings, index terms

This article investigates if and how mobile agents can execute secure electronic transactions on untrusted hosts. An overview of the security issues of mobile agents is first given. The problem of untrusted (i.e., potentially malicious) hosts is one of these issues, and appears to be the most difficult to solve. The current approaches to counter this problem are evaluated, and their relevance for secure electronic transactions is discussed. In particular, a state-of-the-art survey of mobile agen ...

Keywords: Mobile agent security, electronic transactions, malicious hosts

6 A tentative approach to constructing tamper-resistant software

Masahiro Mambo, Takanori Murayama, Eiji Okamoto
January 1998 **Proceedings of the 1997 workshop on New security paradigms NSPW '97**
Publisher: ACM Press

Full text available: pdf(1.05 MB) Additional Information: full citation, references, index terms

7 Security: A framework for trusted instruction execution via basic block signature verification

Milena Milenković, Aleksandar Milenković, Emil Jovanov

April 2004 **Proceedings of the 42nd annual Southeast regional conference ACM-SE 42**

Publisher: ACM Press

Full text available: pdf(276.25 KB) Additional Information: full citation, abstract, references, citings

Most of today's computers are connected to the Internet or at least to a local network, exposing system vulnerabilities to the potential attackers. One of the attackers' goals is the execution of the unauthorized code. In this paper we propose a framework that will allow execution of the trusted code only and prevent malicious code from executing. The proposed framework relies on the run-time verification of basic block signatures. The basic block signatures are generated during a trusted instal ...

Keywords: computer security, intrusion detection, trusted execution

8 Masking the Energy Behavior of DES Encryption

H. Saputra, N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. Brooks, S. Kim, W. Zhang

March 2003 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '03**

Publisher: IEEE Computer Society

Full text available: pdf(264.41 KB) Publisher Site Additional Information: full citation, abstract, citings, index terms

Smart cards are vulnerable to both invasive and non-invasive attacks. Specifically, non-invasive attacks using power and timing measurements to extract the cryptographic key has drawn a lot of negative publicity for smart card usage. The power measurement techniques rely on the data-dependent energy behavior of the underlying system. Further, power analysis can be used to identify the specific portions of the program being executed to induce timing glitches that may in turn help to bypass key ch ...

9 Informal tool demonstrations: A tool for analyzing and detecting malicious mobile code

Akira Mori, Tomonori Izumida, Toshimi Sawada, Tadashi Inoue

May 2006 **Proceeding of the 28th international conference on Software engineering ICSE '06**

Publisher: ACM Press

Full text available: pdf(99.00 KB) Additional Information: full citation, abstract, references, index terms

We present a tool for analysis and detection of malicious mobile code such as computer viruses and internet worms based on the combined use of code simulation, static code analysis, and OS execution emulation. Unlike traditional anti-virus methods, the tool directly inspects the code and identifies commonly found malicious behaviors such as mass mailing, self duplication, and registry overwrite without relying on ``pattern files'' that contain ``signatures'' of previously captured samples. The p ...

Keywords: OS execution emulation, code simulation, malicious code detection, static code analysis

10 Security on the move: indirect authentication using Kerberos

Armando Fox, Steven D. Gribble

November 1996 **Proceedings of the 2nd annual international conference on Mobile**

computing and networking MobiCom '96
Publisher: ACM Press
Full text available: pdf(1.34 MB) Additional Information: full citation, references, citings, index terms

11 Distributed operating systems
Andrew S. Tanenbaum, Robbert Van Renesse
December 1985 **ACM Computing Surveys (CSUR)**, Volume 17 Issue 4
Publisher: ACM Press
Full text available: pdf(5.49 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Distributed operating systems have many aspects in common with centralized ones, but they also differ in certain ways. This paper is intended as an introduction to distributed operating systems, and especially to current university research about them. After a discussion of what constitutes a distributed operating system and how it is distinguished from a computer network, various key design issues are discussed. Then several examples of current research projects are examined in some detail ...

12 Security & privacy: SmartSiren: virus detection and alert for smartphones
Jerry Cheng, Starsky H.Y. Wong, Hao Yang, Songwu Lu
June 2007 **Proceedings of the 5th international conference on Mobile systems, applications and services MobiSys '07**
Publisher: ACM Press
Full text available: pdf(534.00 KB) Additional Information: full citation, abstract, references, index terms

Smartphones have recently become increasingly popular because they provide "all-in-one" convenience by integrating traditional mobile phones with handheld computing devices. However, the flexibility of running third-party softwares also leaves the smartphones open to malicious viruses. In fact, hundreds of smartphone viruses have emerged in the past two years, which can quickly spread through various means such as SMS/MMS, Bluetooth and traditional IP-based applications. Our own implementatio ...

Keywords: alert, privacy, security, smartphone, virus detection

13 Security on FPGAs: State-of-the-art implementations and attacks
Thomas Wollinger, Jorge Guajardo, Christof Paar
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(296.79 KB) Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

14 Defensive techniques: SCUBA: Secure Code Update By Attestation in sensor networks

Arvind Seshadri, Mark Luk, Adrian Perrig, Leendert van Doorn, Pradeep Khosla
September 2006 **Proceedings of the 5th ACM workshop on Wireless security WiSe '06**
Publisher: ACM Press
Full text available: pdf(194.86 KB) Additional Information: full citation, abstract, references, index terms

This paper presents SCUBA (Secure Code Update By Attestation), for detecting and recovering compromised nodes in sensor networks. The SCUBA protocol enables the design of a sensor network that can detect compromised nodes without false negatives, and either repair them through code updates, or revoke the compromised nodes. The SCUBA protocol represents a promising approach for designing secure sensor networks by proposing a first approach for automatic recovery of compromised sensor nodes. The S ...

Keywords: externally-verifiable code execution, secure code update, self-checksumming code, software-based attestation

15 Foundations and applications for secure triggers
Ariel Futoransky, Emiliano Kargieman, Carlos Sarraute, Ariel Waissbein
February 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 1
Publisher: ACM Press
Full text available: pdf(276.02 KB) Additional Information: full citation, abstract, references, index terms

Imagine there is certain content we want to maintain private until some particular event occurs, when we want to have it automatically disclosed. Suppose, furthermore, that we want this done in a (possibly) malicious host. Say the confidential content is a piece of code belonging to a computer program that should remain ciphered and then "be triggered" (i.e., deciphered and executed) when the underlying system satisfies a preselected condition, which must remain secret after code ins ...

Keywords: Malicious host problem, mobile code security, obfuscation, secure triggers, universally composable security

16 A functional taxonomy for software watermarking
Jasvir Nagra, Clark Thomborson, Christian Collberg
January 2002 **Australian Computer Science Communications , Proceedings of the twenty-fifth Australasian conference on Computer science - Volume 4 ACSC '02**, Volume 24 Issue 1
Publisher: Australian Computer Society, Inc., IEEE Computer Society Press
Full text available: pdf(1.19 MB) Additional Information: full citation, abstract, references, cited by, index terms

Despite the recent surge of interest in digital watermarking technology from the research community, we lack a comprehensive and precise terminology for software watermarking. In this paper, we attempt to fill that gap by giving distinctive names for the various protective functions served by software watermarks: Validation Mark, Licensing Mark, Authorship Mark and Fingerprinting Mark. We identify the desirable properties and specific vulnerabilities of each type of watermark, and we illustrate ...

Keywords: authentication, fingerprint, software authorship, software licensing, steganography, watermark

17 Protocol failure in the escrowed encryption standard
Matt Blaze

November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security CCS '94**
Publisher: ACM Press

Full text available: pdf(953.18 KB) Additional Information: full citation, abstract, references, citings, index terms

The Escrowed Encryption Standard (EES) defines a US Government family of cryptographic processors, popularly known as "Clipper" chips, intended to protect unclassified government and private-sector communications and data. A basic feature of key setup between pairs of EES processors involves the exchange of a "Law Enforcement Access Field" (LEAF) that contains an encrypted copy of the current session key. The LEAF is intended to facilitate government access to the cl ...

18 Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency Switching Approach
Shengqi Yang, Wayne Wolf, N. Vijaykrishnan, D. N. Serpanos, Yuan Xie
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(291.83 KB) Additional Information: full citation, abstract, index terms

A novel power attack resistant cryptosystem is presented in this paper. Security in digital computing and communication is becoming increasingly important. Design techniques that can protect cryptosystems from leaking information have been studied by several groups. Power attacks, which infer program behavior from observing power supply current into a processor core, are important forms of attacks. Various methods have been proposed to countermeasure the popular and efficient power attacks. Howe ...

19 Privacy through pseudonymity in user-adaptive systems
Alfred Kobsa, Jörg Schreck
May 2003 **ACM Transactions on Internet Technology (TOIT)**, Volume 3 Issue 2
Publisher: ACM Press

Full text available: pdf(881.69 KB) Additional Information: full citation, abstract, references, citings, index terms, review

User-adaptive applications cater to the needs of each individual computer user, taking for example users' interests, level of expertise, preferences, perceptual and motoric abilities, and the usage environment into account. Central user modeling servers collect and process the information about users that different user-adaptive systems require to personalize their user interaction.Adaptive systems are generally better able to cater to users the more data their user modeling systems collect and ...

Keywords: Chaum mix, KQML, User modeling, access control, anonymity, encryption, personal information, personalization, privacy, pseudonymity, reference model, secrecy, security, user-adaptive systems

20 Robust FPGA intellectual property protection through multiple small watermarks
John Lach, William H. Mangione-Smith, Miodrag Potkonjak
June 1999 **Proceedings of the 36th ACM/IEEE conference on Design automation DAC '99**
Publisher: ACM Press
Full text available: pdf(119.08 KB) Additional Information: full citation, references, citings, index terms

Keywords: field programmable gate array (FPGA), intellectual property protection, watermarking

Results 1 - 20 of 24 Result page: **1** 2 next

Search Results

Results for "(executable module, dummy data, encrypt, decrypt, protect code<in>metadata)" e-mail
Your search matched **8339** of **1625854** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

view selected items Select All Deselect All View: 1-25 | 26-5

1. **Hardware and Binary Modification Support for Code Pointer Protection Fi Overflow**
Tuck, N.; Calder, B.; Varghese, G.;
Microarchitecture, 2004. MICRO-37 2004. 37th International Symposium on
04-08 Dec. 2004 Page(s):209 - 220
Digital Object Identifier 10.1109/MICRO.2004.20
AbstractPlus | Full Text: PDF(296 KB) IEEE CNF
Rights and Permissions

2. **Configurable security protocols for multi-party data analysis with malicio**
Malin, B.; Airoldi, E.; Edoho-Eket, S.; Li, Y.;
Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conferen
5-8 April 2005 Page(s):533 - 544
Digital Object Identifier 10.1109/ICDE.2005.37
AbstractPlus | Full Text: PDF(424 KB) IEEE CNF
Rights and Permissions

3. **Hardware/software IP protection**
Dalpasso, M.; Bogliolo, A.; Benini, L.;
Design Automation Conference, 2000. Proceedings 2000. 37th
June 5-9, 2000 Page(s):593 - 596
AbstractPlus | Full Text: PDF(412 KB) IEEE CNF
Rights and Permissions

4. **A format-compliant configurable encryption framework for access contro**
Jiangtao Wen; Severa, M.; Wenjun Zeng; Luttrell, M.H.; Weiyin Jin;
Circuits and Systems for Video Technology, IEEE Transactions on
Volume 12, Issue 6, June 2002 Page(s):545 - 557
Digital Object Identifier 10.1109/TCSVT.2002.800321
AbstractPlus | Full Text: PDF(394 KB) IEEE JNL
Rights and Permissions

5. **Boosting m-business using a truly secured protocol for data gathering m**
Al-Jaljouli, R.;
Mobile Business, 2005. ICMB 2005. International Conference on
11-13 July 2005 Page(s):537 - 544
Digital Object Identifier 10.1109/ICMB.2005.23

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

AbstractPlus | Full Text: PDF(152 KB) IEEE CNF
Rights and Permissions

6. **Coordinate transformation - a solution for the privacy problem of locatior services?**
Gutscher, A.;
Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th Inter
25-29 April 2006 Page(s):7 pp.
Digital Object Identifier 10.1109/IPDPS.2006.1639681
AbstractPlus | Full Text: PDF(152 KB) IEEE CNF
Rights and Permissions

7. **The hopping ruse**
Chen, M.; Cowie, J.;
Heterogeneous Computing Workshop, 1997. (HCW '97) Proceedings., Sixth
1 April 1997 Page(s):208 - 220
Digital Object Identifier 10.1109/HCW.1997.581422
AbstractPlus | Full Text: PDF(908 KB) IEEE CNF
Rights and Permissions

8. **Analysis of an anonymity network for web browsing**
Rennhard, M.; Rafaeli, S.; LaurentMathy; Plattner, B.; Hutchison, D.;
Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WE
Proceedings. Eleventh IEEE International Workshops on
10-12 June 2002 Page(s):49 - 54
Digital Object Identifier 10.1109/ENABL.2002.1029987
AbstractPlus | Full Text: PDF(287 KB) IEEE CNF
Rights and Permissions

9. **Practical anonymity for the masses with mix-networks**
Rennhard, M.; Plattner, B.;
Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WE
Proceedings. Twelfth IEEE International Workshops on
9-11 June 2003 Page(s):255 - 260
AbstractPlus | Full Text: PDF(300 KB) IEEE CNF
Rights and Permissions

10. **IEEE Std 1364 -2005 IEEE Standard for Verilog Hardware Description Lan**
2006 Page(s):0_1 - 560
AbstractPlus | Full Text: PDF(5970 KB) IEEE STD

11. **Key escrowing today**
Denning, D.E.; Smid, M.;
Communications Magazine, IEEE
Volume 32, Issue 9, Sept. 1994 Page(s):58 - 68
Digital Object Identifier 10.1109/35.312844
AbstractPlus | Full Text: PDF(2192 KB) IEEE JNL
Rights and Permissions

12. **Tracing traitors**
Chor, B.; Fiat, A.; Naor, M.; Pinkas, B.;
Information Theory, IEEE Transactions on
Volume 46, Issue 3, May 2000 Page(s):893 - 910
Digital Object Identifier 10.1109/18.841169
AbstractPlus | References | Full Text: PDF(356 KB) IEEE JNL
Rights and Permissions

13. **Information technology- Telecommunications and information exchange**

systems- Local and metropolitan area networks- Specific requirements- I LAN Medium Access Control (MAC) and Physical Layer (PHY) Specificati
2003 Page(s):i - 513

AbstractPlus | Full Text: PDF(6325 KB) IEEE STD

14. **Mobile Device Security Using Transient Authentication**
Nicholson, A.J.; Corner, M.D.; Noble, B.D.;
Mobile Computing, IEEE Transactions on
Volume 5, Issue 11, Nov. 2006 Page(s):1489 - 1502
Digital Object Identifier 10.1109/TMC.2006.169

AbstractPlus | Full Text: PDF(1648 KB) IEEE JNL
Rights and Permissions

15. **IEEE Standard for Information technology- Telecommunications and info exchange between systems- Local and metropolitan area networks- Spec requirements Part 11: Wireless LAN Medium Access Control (MAC) and F (PHY) specifications Amendment 6: Medium Access Control (MAC) Secu Enhancements**
2004 Page(s):0_1 - 175

AbstractPlus | Full Text: PDF(2342 KB) IEEE STD

16. **Analyzing encryption protocols using formal verification techniques**
Kemmerer, R.A.;
Selected Areas in Communications, IEEE Journal on
Volume 7, Issue 4, May 1989 Page(s):448 - 457
Digital Object Identifier 10.1109/49.17707

AbstractPlus | Full Text: PDF(991 KB) IEEE JNL
Rights and Permissions

17. **Software smart cards via cryptographic camouflage**
Hoover, D.N.; Kausik, B.N.;
Security and Privacy, 1999. Proceedings of the 1999 IEEE Symposium on
9-12 May 1999 Page(s):208 - 215
Digital Object Identifier 10.1109/SECPRI.1999.766915

AbstractPlus | Full Text: PDF(72 KB) IEEE CNF
Rights and Permissions

18. **Integrating the Data Encryption Standard into Computer Networks**
Smid, M.;
Communications, IEEE Transactions on [legacy, pre - 1988]
Volume 29, Issue 6, Jun 1981 Page(s):762 - 772

AbstractPlus | Full Text: PDF(1136 KB) IEEE JNL
Rights and Permissions

19. **Secrecy forever? Analysis of anonymity in Internet-based voting protoco**
Volkamer, M.; Krimmer, R.;
Availability, Reliability and Security, 2006. ARES 2006. The First International
20-22 April 2006 Page(s):8 pp.
Digital Object Identifier 10.1109/ARES.2006.118

AbstractPlus | Full Text: PDF(376 KB) IEEE CNF
Rights and Permissions

20. **Type-based distributed access control**
Chothia, T.; Duggan, D.; Vitek, J.;
Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE
30 June-2 July 2003 Page(s):170 - 184

AbstractPlus | Full Text: PDF(316 KB) IEEE CNF
Rights and Permissions

21. **IEEE trial-use recommended practice for multi-vendor access point inter inter-access point protocol across distribution systems supporting ieee** 2003 Page(s):0_1 - 67
AbstractPlus | Full Text: PDF(543 KB) IEEE STD

22. **The final nail in WEP's coffin**
Bittau, A.; Handley, M.; Lackey, J.;
Security and Privacy, 2006 IEEE Symposium on
21-24 May 2006 Page(s):15 pp.
Digital Object Identifier 10.1109/SP.2006.40
AbstractPlus | Full Text: PDF(376 KB) IEEE CNF
Rights and Permissions

23. **An encryption scheme for limited k-time access to digital media**
Perkins, G.M.; Bhattacharya, P.;
Consumer Electronics, IEEE Transactions on
Volume 49, Issue 1, Feb. 2003 Page(s):171 - 176
Digital Object Identifier 10.1109/TCE.2003.1205472
AbstractPlus | Full Text: PDF(632 KB) IEEE JNL
Rights and Permissions

24. **IEEE Standard for Local and metropolitan area networks Part 16: Air Inte and Mobile Broadband Wireless Access Systems Amendment 2: Physica Access Control Layers for Combined Fixed and Mobile Operation in Lice Corrigendum 1**
2006 Page(s):0_1 - 822
AbstractPlus | Full Text: PDF(5468 KB) IEEE STD

25. **Automatic validation of protocol narration**
Bodei, C.; Buchholtz, M.; Degano, P.; Nielson, F.; Riis Nielson, H.;
Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE
30 June-2 July 2003 Page(s):126 - 140
AbstractPlus | Full Text: PDF(435 KB) IEEE CNF
Rights and Permissions

View: **1-25** | 26-5

Indexed by Inspec®